

THE SYLOW SUBGROUPS OF A FINITE REDUCTIVE GROUP

MICHEL ENGUEHARD AND JEAN MICHEL

Dedicated to professor George Lusztig on the occasion of his 70th birthday

ABSTRACT. We describe the structure of Sylow ℓ -subgroups of a finite reductive group $\mathbf{G}(\mathbb{F}_q)$ when $q \not\equiv 0 \pmod{\ell}$ that we find governed by a complex reflection group attached to \mathbf{G} and ℓ , which depends on ℓ only through the set of cyclotomic factors of the generic order of $\mathbf{G}(\mathbb{F}_q)$ whose value at q is divisible by ℓ . We also tackle the more general case of groups \mathbf{G}^F where F is an isogeny some power of which is a Frobenius morphism.

1. INTRODUCTION

Definition 1.1. *Let \mathbf{G} be a connected reductive group over $\overline{\mathbb{F}}_p$, and F an isogeny such that some power of F is a Frobenius endomorphism; then \mathbf{G}^F is what we call a finite reductive group. To this situation we attach a positive real number q such that for some integer n , the isogeny F^n is the Frobenius endomorphism attached to a \mathbb{F}_{q^n} -structure.*

The goal of this note is to describe the Sylow ℓ -subgroups of \mathbf{G}^F when ℓ is a prime different from p and \mathbf{G} is semisimple. The structure of the Sylow ℓ -subgroups of a Chevalley group was first described by [Gorenstein-Lyons] where they observed that they had a large normal abelian subgroup $(\mathbb{Z}/n)_\ell^a$ where n is the ℓ -part of $\Phi_d(q)$, where d is the multiplicative order of $q \pmod{\ell}$, and they computed a case by case.

In 1992 [Broué-Malle] exhibited subtori of \mathbf{G}^F attached to eigenspaces of elements of the Weyl reflection coset of (\mathbf{G}, F) whose F -stable points are the large abelian groups of [Gorenstein-Lyons]. To these eigenspaces are attached complex reflection groups by Springer's theory.

We show that the structure of the Sylow ℓ -subgroups of \mathbf{G}^F is determined by these complex reflection groups. The results of this note in the case when F is a Frobenius were obtained by the first author in an unpublished note [Enguehard] of 1992; the second author has found a simpler (containing more casefree steps) proof which is an occasion to publish these results. Some of our results appeared also implicitly in [Malle].

The second author wishes to thank Carles Broto for a visit to Barcelona, which started him thinking about this topic.

We thank Raphaël Rouquier for discussions which helped with the proofs of Propositions 2.8 and 2.19(4).

Date: 22nd July 2016.

2010 Mathematics Subject Classification. 20G40, 20D20.

Key words and phrases. reductive groups, Sylow subgroups.

2. THE GENERIC SYLOW THEOREMS

Let \mathbf{G} be as in 1.1; an F -stable maximal torus \mathbf{T} of \mathbf{G} defines the Weyl group $W = N_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$, that we may identify to a reflection subgroup of $\mathrm{GL}(X(\mathbf{T}))$ where $X(\mathbf{T}) := \mathrm{Hom}(\mathbf{T}, \mathbb{G}_m)$, attached to the root system $\Sigma \subset X(\mathbf{T})$ of \mathbf{G} with respect to \mathbf{T} . The isogeny F induces a p -morphism $F^* \in \mathrm{End}(X(\mathbf{T}))$ by the formula $F^*(x) = x \circ F$ for $x \in X(\mathbf{T})$, that is there is a permutation σ of Σ such that for $\alpha \in \Sigma$ we have $F^*(\alpha) = q_\alpha \sigma(\alpha)$ for some power q_α of p ; in particular $F^* \in N_{\mathrm{End}(X(\mathbf{T}))}(W)$.

If q, n are as in 1.1 then F^{*n} is q^n times an element of $\mathrm{GL}(X(\mathbf{T}))$ of finite order, thus over $X(\mathbf{T}) \otimes \mathbb{Z}[q^{-1}]$ we have $F^* = q\phi$ where ϕ is an automorphism of finite order which normalizes W . We call $W\phi$ the *reflection coset associated to (\mathbf{G}, F)* .

Our setting is more general than that of [Broué-Malle] who considered only the special cases where F is a Frobenius endomorphism, or where \mathbf{G}^F is a Ree or Suzuki group. The results of the next subsection allow to extend the definition of Sylow Φ -subtori of [Broué-Malle] to any (\mathbf{G}, F) as in 1.1.

 F -indecomposable tori.

Definition 2.1. For \mathbf{G}, F as in 1.1, a non-trivial subtorus of \mathbf{G} is called F -indecomposable if it is F -stable and contains no proper non-trivial F -stable subtorus.

We say that a group G is an almost direct product of subgroups G_1 and G_2 if they commute, generate G and have finite intersection, and we define similarly an almost direct product of k subgroups by induction on k .

Proposition 2.2. For \mathbf{G}, F as in 1.1, any F -stable subtorus \mathbf{T} of \mathbf{G} is an almost direct product of F -indecomposable tori $\mathbf{S}_1, \dots, \mathbf{S}_k$ and $|\mathbf{T}^F| = |\mathbf{S}_1^F| \dots |\mathbf{S}_k^F|$.

Proof. An F -stable subtorus \mathbf{S} corresponds to a pure F -stable sublattice $X' \subset X := X(\mathbf{T})$ (see for example [Borel, III, Proposition 8.12]). Let d be the smallest power of F which is a split Frobenius, thus on $X(\mathbf{T})$ we have $F^{*d} = q^d \mathrm{Id}$. Let $\pi \in \mathrm{End}(X \otimes \mathbb{Q})$ be a projector on $X' \otimes \mathbb{Q}$. Then in $\mathrm{End}(X \otimes \mathbb{Q})$ we can define the F -invariant projector $\pi' := d^{-1} \sum_{i=1}^d F^{*i} \pi F^{*-i}$ and $\mathrm{Ker} \pi' \cap X$ is another F -stable pure sublattice which after tensoring by \mathbb{Q} becomes a complement to $X' \otimes \mathbb{Q}$. This corresponds to an F -stable subtorus \mathbf{S}' such that $K := \mathbf{S} \cap \mathbf{S}'$ is finite and $\mathbf{T} = \mathbf{S}\mathbf{S}'$. Iterating, we get the first part of the proposition.

The second part of the proposition results from the next two lemmas. □

Lemma 2.3. For \mathbf{G}, F as in 1.1, and K an F -stable finite normal subgroup of \mathbf{G} , then $|(\mathbf{G}/K)^F| = |\mathbf{G}^F|$.

Proof. First, we notice that K is central, thus abelian, since conjugating by \mathbf{G} being continuous must be trivial on K .

Then, the Galois cohomology long exact sequence: $1 \rightarrow K^F \rightarrow \mathbf{G}^F \rightarrow (\mathbf{G}/K)^F \rightarrow H^1(F, K) \rightarrow 1$ shows the result using that $|K^F| = |H^1(F, K)|$. □

Lemma 2.4. Let \mathbf{G} as 1.1 be an almost direct product of F -stable connected subgroups $\mathbf{G} = \mathbf{G}_1 \dots \mathbf{G}_k$. Then $|\mathbf{G}^F| = |\mathbf{G}_1^F| \dots |\mathbf{G}_k^F|$.

Proof. It is enough to consider the case $k = 2$ and then iterate. Thus, we assume $\mathbf{G} = \mathbf{G}_1 \mathbf{G}_2$ where $K = \mathbf{G}_1 \cap \mathbf{G}_2$ is finite. We quotient by K , which makes the product direct, and apply Lemma 2.3 twice. □

Lemma 2.5. *Let \mathbf{S} be an F -indecomposable torus, let η be the smallest power such that $q^\eta \in \mathbb{Z}$, and let d be the smallest power such that $F^{d\eta}$ is a split Frobenius on \mathbf{S} . Let $F^* = q\phi$ on $X(\mathbf{S})$; then the characteristic polynomial Φ of ϕ is a factor in $\mathbb{Z}[x, q^{-1}]$ of $\Phi_d(x^\eta)$, where $\Phi_d(x)$ denotes the d -th cyclotomic polynomial. Further $q^{\deg \Phi} \Phi(x/q) \in \mathbb{Z}[x]$ is irreducible and $|\mathbf{S}^F| = \Phi(q)$.*

Proof. Since $F^{*d\eta}$ acts as $q^{d\eta}$ on $X := X(\mathbf{S})$, the minimal polynomial P of F^* divides $x^{d\eta} - q^{d\eta}$.

The polynomial P is irreducible over \mathbb{Z} , otherwise a proper nontrivial factor P_1 defines an F^* -stable pure proper non-trivial sublattice $\text{Ker}(P_1(F^*))$ of X , which contradicts F -indecomposability of \mathbf{S} .

It follows that X is a $\mathbb{Z}[x]/P$ -module by making x act by F^* , and $X \otimes \mathbb{Q}[x]/P$ is a one-dimensional $\mathbb{Q}[x]/P$ -vector space, otherwise a proper nontrivial subspace would define an F^* -stable pure sublattice of X . It follows that $\dim \mathbf{S} = \deg P = \dim X$ and thus P is also the characteristic polynomial of F^* .

We have in $\mathbb{Z}[x]$ the equality $x^{d\eta} - q^{d\eta} = \prod_{d'|d} (q^{\eta \deg \Phi_{d'}} \Phi_{d'}(x^\eta/q^\eta))$. Since P is irreducible it divides one of the factors, and since $d\eta$ is minimal such that $F^{*d\eta} = q^{d\eta} \text{Id}$, that is minimal such that P divides $x^{d\eta} - q^{d\eta}$, we have that P divides $q^{\eta \deg \Phi_d} \Phi_d(x^\eta/q^\eta)$; equivalently $\Phi = q^{-\deg P} P(qx)$ divides $\Phi_d(x^\eta)$.

We have $|\mathbf{S}^F| = |\text{Irr}(\mathbf{S}^F)| = |X/(F^* - 1)X| = \det(F^* - 1) = (-1)^{\deg P} P(1) = (-q)^{\deg \Phi} \Phi(1/q)$ where the second equality reflects the well known group isomorphism $\text{Irr}(\mathbf{S}^F) \simeq X/(F^* - 1)X$ and the third is a general property of lattices. Finally, since Φ is real and divides $\Phi_d(x^\eta)$, its roots are stable under taking inverses, thus $(-q)^{\deg \Phi} \Phi(1/q) = \Phi(q)$. \square

We call q -cyclotomic the polynomials Φ of Lemma 2.5. In other terms

Definition 2.6. *For q as in 1.1, where q^η is the smallest power of q in \mathbb{Z} , we call q -cyclotomic the monic polynomials $\Phi \in \mathbb{Z}[x, q^{-1}]$ such that $q^{\deg \Phi} \Phi(x/q)$ is a $\mathbb{Z}[x]$ -irreducible factor of some $x^{d\eta} - q^{d\eta}$.*

In the study of semisimple reductive groups we will need the q -cyclotomic polynomials of Lemma 2.7. Note that if d is minimal in Definition 2.6, then Φ is a factor in $\mathbb{Z}[x, q^{-1}]$ of $\Phi_d(x^\eta)$. We are interested in that number d rather than $d\eta$, and to emphasize this we write $\Phi_{\eta,d}$ in the following examples.

Lemma 2.7. *When $q \in \mathbb{Z}$, the q -cyclotomic polynomials are the cyclotomic polynomials.*

When q is an odd power of $\sqrt{2}$, the following polynomials are q -cyclotomic: $\Phi_{2,1}(x) := \Phi_1(x^2)$, $\Phi_{2,2}(x) := \Phi_2(x^2)$, $\Phi_{2,6}(x) := \Phi_6(x^2)$, the factors $\Phi'_{2,4} := x^2 + \sqrt{2}x + 1$ and $\Phi''_{2,4} := x^2 - \sqrt{2}x + 1$ of $\Phi_4(x^2)$, and the factors $\Phi'_{2,12} := x^4 + x^3\sqrt{2} + x^2 + x\sqrt{2} + 1$ and $\Phi''_{2,12} := x^4 - x^3\sqrt{2} + x^2 - x\sqrt{2} + 1$ of $\Phi_{12}(x^2)$.

When q is an odd power of $\sqrt{3}$, the following polynomials are q -cyclotomic: $\Phi_{2,1}(x)$, $\Phi_{2,2}(x)$ and the factors $\Phi'_{2,6} := x^2 + x\sqrt{3} + 1$ and $\Phi''_{2,6} := x^2 - x\sqrt{3} + 1$ of $\Phi_6(x^2)$.

Proof. When $q \in \mathbb{Z}$ the formula $P \mapsto q^{-\deg P} P(qx)$ establishes a bijection between $\mathbb{Z}[x]$ -irreducible factors of $x^d - q^d$ and $\mathbb{Z}[x]$ -irreducible factors of $x^d - 1$, that is cyclotomic polynomials, which gives the first case of the lemma.

For the other cases, we have to check for each given Φ that $q^{\deg \Phi} \Phi(x/q)$ is in $\mathbb{Z}[x]$ and irreducible. \square

Proposition 2.8. *Let $\mathbf{S}, \eta, d, \Phi$ be as in 2.5 and let $P = q^{\deg \Phi} \Phi(x^\eta/q^\eta)$ be the characteristic polynomial of F^* .*

- (1) *Assume that either $q \in \mathbb{Z}$ or that $\mathbb{Z}[x, q^{-\eta}]/P$ is integrally closed. Then $\mathbf{S}^F \simeq \mathbb{Z}/\Phi(q)$.*
- (2) *Let m be a divisor of $\Phi(q)$, and assume either that $d \in \{1, 2\}$ and $q \in \mathbb{Z}$ or that m is prime to $d\eta$; then we have a natural isomorphism $\text{Irr}(\mathbf{S}^F)/m \text{Irr}(\mathbf{S}^F) \simeq \text{Ker}(F^* - 1 \mid X(\mathbf{S})/mX(\mathbf{S}))$.*

Proof. Proceeding as in the proof of Lemma 2.5 we set $X = X(\mathbf{S})$ and $\bar{X} = X/(F^* - 1)X \simeq \text{Irr}(\mathbf{S}^F)$. Letting x act as F^* makes X into a $\mathbb{Z}[x]/P$ -module, and \bar{X} a $\mathbb{Z}[x]/(P, x - 1)$ -module. Since $\mathbb{Z}[x]/(P, x - 1) = \mathbb{Z}/P(1) = \mathbb{Z}/\Phi(q)$ we find that the exponent of \bar{X} divides $\Phi(q)$.

Let $A := \mathbb{Z}[x, q^{-\eta}]/P$. The extension $\mathbb{Z}[x]/P \hookrightarrow A/P$ is flat thus $\bar{X} \otimes_{\mathbb{Z}[x]/P} A \simeq X'/(F^* - 1)X'$ where $X' = X \otimes_{\mathbb{Z}[x]/P} A$; and since the exponent of \bar{X} divides $\Phi(q)$ which is prime to q^η , we have $\bar{X} \simeq \bar{X} \otimes_{\mathbb{Z}[x]/P} A$. Under the assumptions of (1) the ring A is Dedekind: if $\eta \neq 1$ then A is integrally closed thus Dedekind; if $\eta = 1$ then $A \simeq \mathbb{Z}[x, q^{-1}]/\Phi_d$ where the isomorphism is given by $x \mapsto x/q$, and is a localization of the Dedekind ring $\mathbb{Z}[x]/\Phi_d$ by q . Thus X' identifies to a fractional ideal \mathfrak{J} of A and $\bar{X} \simeq \mathfrak{J}/(x - 1)\mathfrak{J}$. If e is the exponent of \bar{X} we have thus $e\mathfrak{J} \subset (x - 1)\mathfrak{J}$, which implies that $x - 1$ divides e in A . This in turn implies that the norm $(-1)^{\deg P} P(1) = \Phi(q)$ of $(x - 1)$ divides e in \mathbb{Z} , thus $e = \Phi(q)$ and $\bar{X} \simeq \mathbb{Z}/\Phi(q)$ and the same isomorphism holds for the dual abelian group \mathbf{S}^F .

For (2), note that by construction $\bar{X}/m\bar{X}$ is the biggest quotient of X on which both $F^* - 1$ and the multiplication by m vanish. It is thus equal to the biggest quotient of X/mX on which $F^* - 1$ vanishes. Thus the question is to see that $\text{Ker}(F^* - 1)$ has a complement in X/mX .

If $q \in \mathbb{Z}$ and $d \in \{1, 2\}$ we have $P = x \pm q$ so $X \simeq \mathbb{Z}$ on which F^* acts by $\mp q$ and $\bar{X} = X/(q \pm 1)$ of which X/mX is a quotient, so $F^* - 1$ vanishes on X/mX which is thus equal to $\bar{X}/m\bar{X}$ and there is nothing to prove.

Assume now m prime to $d\eta$. There exists $R \in \mathbb{Z}[x]$ such that in $\mathbb{Z}[x]$ we have $P = (x - 1)R + P(1)$. Taking derivatives, we get $P' = (x - 1)R' + R$, whence $R(1) = P'(1)$. Let δ be the discriminant of P ; we can find polynomials $M, N \in \mathbb{Z}[x]$ such that $MP + NP' = \delta$, which evaluating at 1 gives $M(1)P(1) + N(1)P'(1) = \delta$. Since q is prime to $P(1)$, thus to m , and δ is a divisor of the discriminant of $X^{d\eta} - q^{d\eta}$, equal to $q^{d\eta(d\eta-1)}(d\eta)^{d\eta}$, thus prime to m , we find that $P'(1)$ is prime to m . In $(\mathbb{Z}/m)[x]$ we have $P = (x - 1)R$, thus applied to F^* we get that on X/mX we have $0 = P(F^*) = (F^* - 1)R(F^*)$, whence $\text{Ker}(F^* - 1) + \text{Ker}(R(F^*)) = X/mX$. Since $R(1)$ is prime to m , we can write $1 \equiv Q(x - 1) + aR$ in $(\mathbb{Z}/m)[x]$ for some $Q \in (\mathbb{Z}/m)[x]$ and a the inverse (mod m) of $R(1)$. This proves that $\text{Ker}(F^* - 1) \cap \text{Ker}(R(F^*)) = 0$ thus X/mX is the direct sum of $\text{Ker}(F^* - 1)$ and $\text{Ker}(R(F^*))$ q.e.d. \square

Complex reflection cosets. (1) to (3) below are classical results of Springer and Lehrer.

Proposition 2.9. *Let V be a finite dimensional vector space over a subfield k of \mathbb{C} , let $W \subset \text{GL}(V)$ be a finite complex reflection group and let $\phi \in N_{\text{GL}(V)}(W)$, so that $W\phi$ is a reflection coset; let $(d_1, \varepsilon_1), \dots, (d_n, \varepsilon_n)$ be its generalized degrees (see for instance [Broué, 4.2]). For ζ a root of unity define $a(\zeta)$ as the multiset of the d_i such that $\zeta^{d_i} = \varepsilon_i$. Then:*

- (1) For any root of unity ζ , the maximum dimension when $w\phi$ runs over $W\phi$ of a ζ -eigenspace of $w\phi$ on $V \otimes_k k[\zeta]$ is $|a(\zeta)|$.
- (2) For $w\phi \in W\phi$ denote $V_{w,\zeta} \subset V \otimes_k k[\zeta]$ its ζ -eigenspace. Assume $\dim V_{w,\zeta} = |a(\zeta)|$ and let $C = C_W(V_{w,\zeta})$ and $N = N_W(V_{w,\zeta})$. Then N/C is a complex reflection group acting on $V_{w,\zeta}$, with reflection degrees $a(\zeta)$.
- (3) Any two subspaces $V_{w,\zeta}$ and $V_{w',\zeta}$ of dimension $|a(\zeta)|$ are W -conjugate.
- (4) For $w\phi$ as in (2) the natural actions of $w\phi$ on N and C induce the trivial action on N/C .
- (5) Let $a \in \mathbb{Z}$ be such that $(W\phi)^a = W\phi$ and such that ζ and ζ^a are conjugate by $\text{Gal}(k[\zeta]/k)$. Then for $w\phi$ as in (2) there exists $v \in N_W(N) \cap N_W(C)$ which conjugates $w\phi C$ to $(w\phi)^a C$.

Proof. For (1) see for instance [Broué, 5.2], for (2) see [Broué, 5.6(3) and (4)] and for (3) see [Broué, 5.6 (1)]. (4) results from the observation that if $n \in N$ and $v \in V_{w,\zeta}$ then $(n^{-1} \cdot {}^{w\phi}n)(v) = (n^{-1}w\phi n(w\phi)^{-1})(v) = (n^{-1}w\phi n)(\zeta^{-1}v) = (n^{-1}w\phi)(\zeta^{-1}n(v)) = (n^{-1})(n(v)) = v$ thus $n^{-1} \cdot {}^{w\phi}n \in C$.

For (5), $\text{Gal}(k[\zeta]/k)$ acts naturally on $V \otimes_k k[\zeta]$, commuting with $\text{GL}(V)$, in particular with W and ϕ . If $\sigma \in \text{Gal}(k[\zeta]/k)$ is such that $\sigma(\zeta) = \zeta^a$, let $\zeta^{a'} = \sigma^{-1}(\zeta)$. Then $\sigma^{-1}(V_{w,\zeta}) = V_{w,\zeta^{a'}}$. It follows that $N = N_W(V_{w,\zeta^{a'}})$ and $C = C_W(V_{w,\zeta^{a'}})$.

Now since a' is the inverse of a modulo the order of ζ the space $V_{w,\zeta^{a'}}$ is the ζ -eigenspace of $(w\phi)^a$. By assumption we have $(w\phi)^a \in W\phi$. Since two maximal ζ -eigenspaces of elements of $W\phi$ are conjugate by (3) there exists $v \in W$ which conjugates $V_{w,\zeta}$ to $V_{w,\zeta^{a'}}$, and $v \in N_W(N) \cap N_W(C)$ since $N = N_W(V_{w,\zeta^{a'}})$ and $C = C_W(V_{w,\zeta^{a'}})$. The element v thus conjugates the set $w\phi C$ of elements which have $V_{w,\zeta}$ as ζ -eigenspace to the set $(w\phi)^a C$ of elements which have $V_{w,\zeta^{a'}}$ as ζ -eigenspace. \square

Generic Sylow subgroups. We define the Sylow Φ -subtori of (\mathbf{G}, F) , first in the case when \mathbf{G} is quasi-simple, then in the case of descent of scalars.

From now on we assume \mathbf{G} semisimple. Then, if $(d_1, \varepsilon_1), \dots, (d_n, \varepsilon_n)$ are the generalized degrees of the reflection coset $W\phi$, we have (see [Steinberg, 11.16])

$$(2.10) \quad |\mathbf{G}^F| = q^{\sum_i (d_i - 1)} \prod_i (q^{d_i} - \varepsilon_i).$$

Proposition 2.11. *Let \mathbf{G} be as in 1.1 and quasi-simple. Then we can rewrite the order formula 2.10 for $|\mathbf{G}^F|$ as*

$$(2.12) \quad |\mathbf{G}^F| = q^{\sum_i (d_i - 1)} \prod_{\Phi \in \mathcal{P}} \Phi(q)^{n_\Phi}$$

where \mathcal{P} is a set of q -cyclotomic polynomials, and where $0 \neq n_\Phi = |a(\zeta)|$ (see 2.9) for any root ζ of Φ . For each $\Phi \in \mathcal{P}$ there exists a non-trivial F -stable subtorus \mathbf{S}_Φ of \mathbf{G} such that $|\mathbf{S}_\Phi^F| = \Phi(q)^{n_\Phi}$.

We note that if \mathbf{G}^F is a Ree or Suzuki group, the η of Definition 2.6 is 2. Otherwise $\eta = 1$ and the q -cyclotomic polynomials are cyclotomic polynomials.

We call any F -stable torus \mathbf{S} such that $|\mathbf{S}^F|$ is a power of $\Phi(q)$ a Φ -torus, and tori \mathbf{S}_Φ as above are called *Sylow Φ -subtori* of (\mathbf{G}, F) — we abuse notation and call

them Sylow Φ -subtori of \mathbf{G} when F is clear from the context; they are the almost direct product of n_Φ F -indecomposable Φ -tori.

Proof. Proposition 2.11 is essentially in [Broué-Malle] but let us reprove it.

First, we note that assuming $|\mathbf{G}^F|$ has a decomposition of the form 2.12, the value of n_Φ results from 2.10: let ζ be any root of $\Phi(x)$. Then $(x - \zeta)$ divides $\Phi(x)$ with multiplicity one, and does not divide any another $\Phi'(x)$ for $\Phi' \in \mathcal{P}$ since the $\Phi(x/q)$ are distinct irreducible polynomials in $\mathbb{Q}[x]$. Thus n_Φ is the number of pairs (d_i, ε_i) such that $x - \zeta$ divides $x^{d_i} - \varepsilon_i$.

There is a decomposition of the form 2.12: if $\eta = 1$ we get such a decomposition of $|\mathbf{G}^F|$ by decomposing each term of 2.10 into a product of cyclotomic polynomials. Otherwise \mathbf{G}^F is a Ree or Suzuki group, $\eta = 2$ and q is an odd power of $\sqrt{2}$ or $\sqrt{3}$, and the set \mathcal{P} and the decomposition of the form 2.12 is given by what follows:

(\mathbf{G}, F)	$ \mathbf{G}^F $	generalized degrees of $W\phi$
${}^2B_2(q^2)$	$q^4(\Phi_{2,1}\Phi'_{2,4}\Phi''_{2,4})(q)$	$\{(2, 1), (4, -1)\}$
${}^2F_4(q^2)$	$q^{24}(\Phi_{2,1}^2\Phi_{2,2}^2\Phi_{2,4}^2\Phi_{2,6}^2\Phi_{2,12}^2\Phi_{2,12}'')(q)$	$\{(2, 1), (6, -1), (8, 1), (12, -1)\}$
${}^2G_2(q^2)$	$q^6(\Phi_{2,1}\Phi_{2,2}\Phi_{2,6}'\Phi_{2,6}'')(q)$	$\{(2, 1), (6, -1)\}$

Note that for $\eta = 2$ our “ q -cyclotomic polynomials” are the “ (tp) -cyclotomic polynomials” defined in [Broué-Malle, 3.14].

To construct the torus \mathbf{S}_Φ for $\Phi \in \mathcal{P}$, let us choose ζ a root of Φ and w as in (2) of Proposition 2.9. Then if \mathbf{T}_w is a maximal torus of type w with respect to \mathbf{T} , so that $(\mathbf{T}_w, F) \simeq (\mathbf{T}, wF)$, the characteristic polynomial of $w\phi$ on $X(\mathbf{T})$ has $\Phi(x)^{n_\Phi}$ as a factor; the kernel of $\Phi(w\phi)$ on $X(\mathbf{T})$ is a pure sublattice corresponding to a subtorus \mathbf{S}_Φ of \mathbf{T}_w such that $|\mathbf{S}_\Phi^F| = \Phi(q)^{n_\Phi}$. \square

Proposition 2.13. *Let (\mathbf{G}, F) be as in 1.1, semisimple and such that the Dynkin diagram of \mathbf{G} has n connected components permuted transitively by F . Then there exists a reductive group \mathbf{G}_1 with isogeny F_1 such that up to isomorphism \mathbf{G} is a “descent of scalars” $\mathbf{G} = \mathbf{G}_1^n$ with $F(g_1, \dots, g_n) = (g_2, \dots, g_n, F_1(g_1))$.*

Then $\mathbf{G}^F \simeq \mathbf{G}_1^{F_1}$, and if the scalar associated to (\mathbf{G}, F) is q that associated to (\mathbf{G}_1, F_1) is $q_1 := q^n$. Thus we have $|\mathbf{G}^F| = q^{n \sum_i (d_i - 1)} \prod_{\Phi \in \mathcal{P}} \Phi(q^n)^{n_\Phi}$ where d_i, \mathcal{P}, n_Φ are as given by 2.11 for (\mathbf{G}_1, F_1, q_1) .

Here again, for $\Phi \in \mathcal{P}$ there exists a Sylow Φ -subtorus of \mathbf{G} , that is an F -stable subtorus \mathbf{S}_Φ such that $|\mathbf{S}_\Phi^F| = \Phi(q^n)^{n_\Phi}$.

Proof. The proposition is obvious apart perhaps for the statement about the existence of \mathbf{S}_Φ . This results in particular from the following lemma that we need for future reference.

Lemma 2.14. *In the situation of Proposition 2.13, let (\mathbf{T}, wF) where $\mathbf{T} = \mathbf{T}_1^n$ be a maximal torus of type $w = (1, \dots, 1, w_1)$ of \mathbf{G} and define ϕ on $V = X(\mathbf{T}) \otimes \mathbb{C}$ (resp. ϕ_1 on $V_1 = X(\mathbf{T}_1) \otimes \mathbb{C}$) by $F^* = q\phi$ (resp. $F_1^* = q_1\phi_1$). Then if the characteristic polynomial of $w_1\phi_1$ is $P(x)$, that of $w\phi$ is $P(x^n)$. Let Φ be a q_1 -cyclotomic factor of P (corresponding to a $\mathbb{Z}[x]$ -irreducible factor of the characteristic polynomial of $w_1F_1^*$) and let ζ be a root of $\Phi(x^n)$. Denote by V_ζ the ζ -eigenspace of $w\phi$ (resp. by V_{1,ζ^n} the ζ^n -eigenspace of $w_1\phi_1$).*

Let \mathbf{S}_1 be the Sylow Φ -subtorus of (\mathbf{G}_1, F_1) determined by $\text{Ker}(\Phi(w_1\phi_1))$, and \mathbf{S} be the wF -stable subtorus of \mathbf{T} determined by $\text{Ker}(\Phi((w\phi)^n))$. Then \mathbf{S} is a Sylow

Φ -subtorus of (\mathbf{G}, F) and

$$N_W(V_\zeta)/C_W(V_\zeta) \simeq N_{W_1}(V_{1,\zeta^n})/C_{W_1}(V_{1,\zeta^n}) \simeq N_{\mathbf{G}_1}(\mathbf{S}_1)/C_{\mathbf{G}_1}(\mathbf{S}_1) \simeq N_{\mathbf{G}}(\mathbf{S})/C_{\mathbf{G}}(\mathbf{S})$$

and we have an isomorphism $\mathbf{S}^{wF} \simeq \mathbf{S}_1^{w_1 F_1}$ compatible with the actions of $N_{\mathbf{G}}(\mathbf{S})/C_{\mathbf{G}}(\mathbf{S})$ and $N_{\mathbf{G}_1}(\mathbf{S}_1)/C_{\mathbf{G}_1}(\mathbf{S}_1)$ and the above isomorphism.

Proof. Let $X = X(\mathbf{T})$, $X_1 = X(\mathbf{T}_1)$. On $X \simeq X_1^n$ we have $F^*(x_1, \dots, x_n) = (x_2, \dots, x_n, F_1^*(x_1))$, thus $\phi(x_1, \dots, x_n) = (q^{-1}x_2, \dots, q^{-1}x_n, q_1 q^{-1}x_1)$. It follows by an easy computation that V_ζ is equal to the set of $(x, (q\zeta)x, \dots, (q\zeta)^{n-1}x)$ where $x \in V_{1,\zeta^n}$, that $C_W(V_\zeta) = \{(v_1, \dots, v_n) \mid v_i \in C_{W_1}(V_{1,\zeta^n})\}$ and that $N_W(V_\zeta) = \{(vv_1, \dots, vv_n) \mid v \in N_{W_1}(V_{1,\zeta^n}), v_i \in C_{W_1}(V_{1,\zeta^n})\}$. This shows that $N_W(V_\zeta)/C_W(V_\zeta) \simeq N_{W_1}(V_{1,\zeta^n})/C_{W_1}(V_{1,\zeta^n})$. Since when ζ runs over the roots of $\Phi(x^n)$ the $q_1\zeta^n$ are roots of the same $\mathbb{Z}[x]$ -irreducible polynomial $q_1^{\deg \Phi} \Phi(x/q_1)$, the ζ^n are Galois conjugate thus $C_{W_1}(V_{1,\zeta^n})$ (resp. $N_{W_1}(V_{1,\zeta^n})$) centralizes (resp. normalizes) all the conjugate eigenspaces, whence our claim that $N_{W_1}(V_{1,\zeta^n})/C_{W_1}(V_{1,\zeta^n}) \simeq N_{\mathbf{G}_1}(\mathbf{S}_1)/C_{\mathbf{G}_1}(\mathbf{S}_1)$. Now $\text{Ker}(\Phi((w\phi)^n))$ is the span of V_ζ for all roots ζ of $\Phi(x^n)$ and by the analysis above $C_W(V_\zeta)$ and $N_W(V_\zeta)$ are independent of ζ , thus isomorphic to $C_W(\mathbf{S})$ and $N_W(\mathbf{S})$.

We have the following commutative diagram

$$\begin{array}{ccccc} X & \xrightarrow{wF^*-1} & X & \xrightarrow{\text{Res}} & \text{Irr}(\mathbf{T}^{wF}) \longrightarrow 1 \\ \downarrow \Sigma & & \downarrow \Sigma & & \downarrow \sim \\ X_1 & \xrightarrow{w_1 F_1^*-1} & X_1 & \xrightarrow{\text{Res}} & \text{Irr}(\mathbf{T}_1^{w_1 F_1}) \longrightarrow 1 \end{array}$$

where Σ is the map $(x_1, \dots, x_n) \mapsto x_1 + \dots + x_n$. Since we have $\Sigma \circ (wF)^n = w_1 F_1 \circ \Sigma$, for any polynomial Q the morphism Σ induces a surjective morphism $\text{Ker}(Q((wF^*)^n)) \rightarrow \text{Ker}(Q(w_1 F_1^*))$ whence for $Q = P$ a surjection $\text{Irr}(\mathbf{S}^{wF}) \rightarrow \text{Irr}(\mathbf{S}_1^{w_1 F_1})$; since $|\mathbf{S}^{wF}|$ is prime to $|\mathbf{T}^{wF}/\mathbf{S}^{wF}|$ this surjection must be an isomorphism. Extended to $V = X \otimes \mathbb{C}$, the map Σ sends V_ζ to V_{1,ζ^n} and sends the action of $N_W(V_\zeta)/C_W(V_\zeta)$ to that of $N_{W_1}(V_{1,\zeta^n})/C_{W_1}(V_{1,\zeta^n})$, whence the last statement of the lemma. \square

Note that any element of $W\phi$ is conjugate to an element of the form $(1, \dots, 1, w_1)\phi_1$ so the form of w in the statement of Lemma 2.14 covers all the types of maximal tori. \square

Remark 2.15. If the generalized degrees of $W_1\phi_1$ are $(d_i, \varepsilon_i)_i$ those of $W\phi$ are $(d_i, \eta_{i,j})$ where $\eta_{i,j}$ for $j \in \{1, \dots, n\}$ runs over the n -th roots of ε_i . It follows that n_Φ can be defined in terms of $W\phi$ as it is also the number of $(d_i, \eta_{i,j})$ such that $\zeta^{d_i} = \eta_{i,j}$, where ζ is any root of $\Phi(x^n)$.

Remark 2.16. For $\Phi \in \mathcal{P}(\mathbf{G})$, a Sylow Φ -subtorus of \mathbf{G} is a “power” of a subtorus \mathbf{S}_0 such that $|\mathbf{S}_0^F| = \Phi(q)$. If \mathbf{G} is quasi-simple, such a subtorus \mathbf{S}_0 is F -indecomposable (since then the polynomial Φ is q -cyclotomic). But this is no longer true for a descent of scalars. First, a cyclotomic polynomial in x^n decomposes in several cyclotomic polynomials according to the formula $\Phi_d(x^n) = \prod_{\{\mu \mid n, \frac{n}{\mu} \text{ prime to } d\}} \Phi_{\mu d}(x)$ (see [Broué-Malle, Appendice 2]). But there could be further decompositions: for instance, the characteristic polynomial of F^* on a Coxeter torus of a semisimple group \mathbf{G} of type B_2 over \mathbb{F}_2 is $x^2 + 4$, which is \mathbb{Z} -irreducible. But on a descent of scalars $\mathbf{G} \times \mathbf{G}$, the characteristic polynomial

of F^* on a lift of scalars of this torus is $x^4 + 4$ which is no longer \mathbb{Z} -irreducible: $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$, so the torus seen inside the descent of scalars is no longer F -indecomposable.

We could have decomposed $|\mathbf{G}^F|$ into a product of q -cyclotomic polynomials corresponding to F -indecomposable tori, but in the case of descent of scalars it was convenient to use larger tori.

Remark 2.17. An arbitrary semisimple reductive group is of the form $\mathbf{G} = \mathbf{G}_1 \dots \mathbf{G}_k$, an almost direct product of descents of scalars of quasi-simple groups \mathbf{G}_i , corresponding to the orbits of F on the connected components of the Dynkin diagram of \mathbf{G} . Then we have $|\mathbf{G}^F| = |\mathbf{G}_1^F| \dots |\mathbf{G}_k^F|$ by Lemma 2.4, and similarly, if \mathbf{S} is an F -stable torus of \mathbf{G} , and $\mathbf{S}_i = \mathbf{S} \cap \mathbf{G}_i$, then $|\mathbf{S}^F| = |\mathbf{S}_1^F| \dots |\mathbf{S}_k^F|$. This can be used to give a global decomposition of $|\mathbf{G}^F|$, but the polynomials \mathcal{P} in one factor could divide those in another. For instance we could have $\Phi'_{2,4}$ for a factor of \mathbf{G} of type 2B_2 and Φ_8 for another factor of type B_2 . Because of this it is cumbersome to give a global statement.

From now on we fix (\mathbf{G}, F) as in 2.13, which determines q, n , and η minimal such that $q^{n\eta} \in \mathbb{Z}$. This allows in the next definition to omit the mention of \mathbf{G} and F from the notation $d(\ell)$.

Definition 2.18. Let ℓ be a prime number different from p . In the context of 2.13 we define $d(\ell)$ as the order of $q^{n\eta} \pmod{\ell}$ ($\pmod{4}$ if $\ell = 2$).

In particular $\ell | \Phi_{d(\ell)}(q^{n\eta})$.

The next proposition extends some of the Sylow theorems of [Broué-Malle], and introduces a complex reflection group W_Φ attached to each Φ in the set \mathcal{P} of 2.11.

Proposition 2.19. Under the assumptions of 2.13, let \mathbf{T} be an F -stable maximal torus of \mathbf{G} in an F -stable Borel subgroup, and let $W_\Phi \subset \mathrm{GL}(X(\mathbf{T}))$ be the reflection coset associated to (\mathbf{G}, F) . Then for each $\Phi \in \mathcal{P}$:

- (1) If ζ is a root of $\Phi(x^n)$ and w is as in 2.9(2), a maximal torus of \mathbf{G} of type w with respect to \mathbf{T} contains a unique Sylow Φ -subtorus \mathbf{S} .

For ζ, w as in (1) let $W_\Phi = N_W(V_\zeta)/C_W(V_\zeta)$ where V_ζ is the ζ -eigenspace of $w\phi$ on $V = X(\mathbf{T}) \otimes \mathbb{C}$.

- (2) For \mathbf{S} as in (1) we have $N_{\mathbf{G}^F}(\mathbf{S})/C_{\mathbf{G}^F}(\mathbf{S}) = N_{\mathbf{G}}(\mathbf{S})/C_{\mathbf{G}}(\mathbf{S}) \simeq W_\Phi$, and W_Φ can be identified to a subgroup of $\mathrm{GL}(X(\mathbf{S}))$.
- (3) The Sylow Φ -tori of \mathbf{G} are \mathbf{G}^F -conjugate.
- (4) Let $\ell \neq p$ be a prime number, and assume that Φ divides $\Phi_{d(\ell)}$ (see Definition 2.18). Then unless $\ell = 2$ and (\mathbf{G}_1, F_1) is of type 2G_2 , any Sylow ℓ -subgroup of W_Φ acts faithfully on the subgroup of ℓ -elements \mathbf{S}_ℓ^F of \mathbf{S}^F .

Proof. For (1) we consider a torus (\mathbf{T}, wF) of type w . Then a wF -stable subtorus corresponds to the span of a subset of eigenspaces of $w\phi$ on V . Since the polynomials Φ are prime to each other the polynomials $\Phi(x^n)$ are also, thus $q\zeta$ is root of no other factor of the characteristic polynomial of $w\phi$ than $\Phi(x^n)$. Thus the \mathbf{S} defined in Lemma 2.14, which we will denote \mathbf{S}_0 , is unique.

Let us show (2). Let $(\mathbf{T}_w, F, \mathbf{S})$ be conjugate to $(\mathbf{T}, wF, \mathbf{S}_0)$. Let $\mathbf{L} = C_{\mathbf{G}}(\mathbf{S})$, which, as the centralizer of a torus, is a Levi subgroup. Then we note that $N_{\mathbf{G}}(\mathbf{S}) \subset N_{\mathbf{G}}(\mathbf{L})$. It follows that we can find representatives of $N_{\mathbf{G}}(\mathbf{S})$ modulo \mathbf{L} in $N_{\mathbf{G}}(\mathbf{T}_w)$ since for $n \in N_{\mathbf{G}}(\mathbf{S})$ the torus ${}^n\mathbf{T}_w$ is another maximal torus of \mathbf{L} which

is thus \mathbf{L} -conjugate to \mathbf{T}_w . We thus get that $N_{\mathbf{G}}(\mathbf{S})/\mathbf{L} = N_{\mathbf{G}}(\mathbf{S}, \mathbf{T}_w)/(N_{\mathbf{G}}(\mathbf{T}_w) \cap \mathbf{L})$; transferring this to \mathbf{T} and then to W we get $N_{\mathbf{G}}(\mathbf{S}, \mathbf{T}_w)/(N_{\mathbf{G}}(\mathbf{T}_w) \cap \mathbf{L}) \simeq N_W(\mathbf{S}_0)/C_W(\mathbf{S}_0)$ where \mathbf{S}_0 is the subtorus of \mathbf{T} determined by $\text{Ker}(P(wF^*))$ where $P = \Phi(x^n/q^n)$. The action of F is transferred to the action of $w\phi$ on this quotient.

That $N_W(\mathbf{S}_0) = N_W(V_\zeta)$ and $C_W(\mathbf{S}_0) = C_W(V_\zeta)$ was given in 2.14.

By 2.9(4) we see that the action of $w\phi$ on $N_W(\mathbf{S}_0)/C_W(\mathbf{S}_0)$ is trivial, thus also that of F on $N_{\mathbf{G}}(\mathbf{S})/C_{\mathbf{G}}(\mathbf{S})$, thus $N_{\mathbf{G}}(\mathbf{S})/C_{\mathbf{G}}(\mathbf{S}) = (N_{\mathbf{G}}(\mathbf{S})/C_{\mathbf{G}}(\mathbf{S}))^F = N_{\mathbf{G}}(\mathbf{S})^F/C_{\mathbf{G}}(\mathbf{S})^F = N_{\mathbf{G}^F}(\mathbf{S})/C_{\mathbf{G}^F}(\mathbf{S})$, the second equality since $\mathbf{L} = C_{\mathbf{G}}(\mathbf{S})$ is connected. Finally, the last part of (2) results from the fact that the representation of W_Φ on $X(\mathbf{S}_0)$, extended to $X(\mathbf{S}_0) \otimes \mathbb{C}$ has as summand the representation of W_Φ on V_ζ , which is the reflection representation, thus faithful.

(3) is a direct translation of 2.9(3): when brought to subtori of \mathbf{T} corresponding to eigenspaces of $w\phi$ (resp. $w'\phi$) the \mathbf{G}^F -conjugacy of two Sylow Φ -subtori corresponds to the W -conjugacy of the corresponding eigenspaces.

For (4) we first remark that we can reduce to the case where \mathbf{G} is quasi-simple, using 2.14. Thus either $q \in \mathbb{Z}$ or \mathbf{G}^F is a Ree or a Suzuki group. Let δ be the order of the coset $W\phi$, that is the smallest integer such that $(W\phi)^\delta = W$. We have $\delta \in \{1, 2, 3\}$. We first show the

Lemma 2.20. *If \mathbf{G} is quasi-simple and we are in one of the cases:*

- (1) $q \in \mathbb{Z}$ and $\delta \in \{1, 2\}$.
- (2) $q \in \mathbb{Z}$, $\delta = 3$ and d is prime to 3.
- (3) q is an odd power of $\sqrt{2}$ and $\ell = 3$.

then W_Φ acts faithfully on \mathbf{S}_ℓ^F .

Proof. On $X(\mathbf{T}) \otimes \mathbb{Q}(q^{-1})$ we have $wF^* = qw\phi$. The characteristic polynomial Q of wF^* on $X(\mathbf{S})$ is $q^{n_\Phi \deg \Phi} \Phi(x/q)^{n_\Phi}$; as wF^* is semisimple, the minimal polynomial of wF^* is $P = q^{\deg \Phi} \Phi(x/q)$. We can identify $X(\mathbf{S})$ with $\text{Ker}(P(qw\phi))$ on $X(\mathbf{T})$. As in the proof of Proposition 2.8, if $X = X(\mathbf{S})$ we can make $X' = X \otimes \mathbb{Z}[q^{-1}]$ an A -module where $A = \mathbb{Z}[x, q^{-\eta}]/P$. Under the assumptions of the lemma A is a Dedekind ring. This results from the proof of 2.8(1) when $q \in \mathbb{Z}$. In the remaining case (3) of Lemma 2.20, $\eta = 2$ and the order of $q^2 \pmod{3}$ is 2, thus $\Phi = x^2 + 1$ and $P = x^2 + q^2$; we have $A = \mathbb{Z}[x, q^{-2}]/P \simeq \mathbb{Z}[1/2, \sqrt{-2}]$ which is integrally closed (thus Dedekind) since localized of $\mathbb{Z}[\sqrt{-2}]$ which is integrally closed. As an A -module of rank n_Φ , the module X' is a sum of projective rank 1 submodules thus \mathbf{S} is a product of n_Φ copies of a wF -indecomposable torus. By Proposition 2.19(2) we can identify W_Φ to a subgroup of $\text{GL}(X)$. With the notations of 2.8, since the assumption of 2.8(1) is satisfied, $\bar{X} := X/(wF^* - 1)X \simeq \text{Irr}(\mathbf{S}^{wF})$ is isomorphic to $(\mathbb{Z}/\Phi(q))^{n_\Phi}$. The representation of W_Φ on X reduces to \bar{X} . We will show it is faithful on $\bar{X}/\ell\bar{X}$ (or $\bar{X}/4\bar{X}$ when $\ell = 2$).

If $q \in \mathbb{Z}$ and $\ell = 2$ then $d \in \{1, 2\}$ and we can apply Proposition 2.8(2) taking $m = 4$. We get that $\bar{X}/4\bar{X} \simeq \text{Ker}(wF^* - 1 \mid X/4X)$. We have as observed in the proof of Proposition 2.8 that $\text{Ker}(wF^* - 1) = X/4X$ and the representation of W_Φ on $\bar{X}/4\bar{X}$, which is a quotient of $\text{Irr}(\mathbf{S}_\ell^{wF})$, is faithful by Lemma 4.3.

If $q \in \mathbb{Z}$ and $\ell \neq 2$ then d is prime to ℓ ; and in case (3) of Lemma 2.20 $\eta = 2$, $\ell = 3$ thus $d = 2$ and ℓ is prime to $d\eta$. In both cases we can apply Proposition 2.8(2) with $m = \ell$ to get that $\bar{X}/\ell\bar{X} \simeq \text{Ker}(wF^* - 1 \mid X/\ell X)$. We know by Lemma 4.3 that the representation of W_Φ on $X/\ell X$ is faithful and we would like to conclude that it is faithful on the submodule $\text{Ker}(wF^* - 1)$. We use the element v given

by Proposition 2.9(5): it preserves the kernel of $\Phi(w\phi)$ thus induces an element of $\mathrm{GL}(X)$ which defines an automorphism σ of W_Φ which sends $w\phi$ to $(w\phi)^a$, so it remains true after reduction $(\bmod \ell)$ that σ sends $w\phi$ to $(w\phi)^a$, thus permutes the eigenspaces of wF^* on $X/\ell X$: since d is the order of $q \pmod{\ell}$, all the primitive d -th roots of unity live in \mathbb{F}_ℓ and the eigenvalues of wF^* are the product of one primitive d -th root of unity, which is q , by the other primitive d -th roots of unity so are of the form q^{1-a} where a runs over $(\mathbb{Z}/d)^\times$. And under the assumption $(W\phi)^a = W\phi$ of 2.9(5) we can find v thus σ which sends the q^{1-a} -eigenspace of wF^* to the $q^{1-1} = 1$ -eigenspace.

If every a prime to d has a representative in $1 + \delta\mathbb{Z}$ we can satisfy $(W\phi)^a = W\phi$ for such a thus every eigenspace is isomorphic as a W_Φ -module to $\mathrm{Ker}(wF^* - 1)$. Then W_Φ is faithful on the whole $X/\ell X$ if and only if it is faithful on $\mathrm{Ker}(wF^* - 1)$, thus we conclude. If $a \equiv 1 \pmod{\gcd(d, \delta)}$ then by Bezout's theorem there exist integers α, β such that $a = 1 + \alpha d + \beta \delta$, and then $a - \alpha d \in 1 + \delta\mathbb{Z}$ is a representative of a .

If $\delta = 1$ or $\delta = 2$ then every a prime to d is $\equiv 1 \pmod{\gcd(d, \delta)}$ and we conclude. We conclude similarly if $\delta = 3$ and d is prime to 3, or in case (3) of Lemma 2.20 since in this case $d = 2$. \square

When $q \in \mathbb{Z}$ the only case not covered by the lemma is 3D_4 and d divisible by 3, that is $d \in \{3, 6, 12\}$. But in this case $\ell > 3$, since d is the order of $q \pmod{\ell}$, thus $|W|$ is prime to ℓ and a fortiori the Sylow ℓ -subgroup of W_Φ is trivial.

For the Ree and Suzuki groups we do not have to consider 2B_2 since W is a 2-group and $\ell \neq p$, and the groups 2G_2 since only the prime $\ell = 2$ divides $|W|$ and is different from p , and this case is excluded in the proposition.

For the groups 2F_4 the only prime $\ell \neq p$ such that $\ell || |W|$ is $\ell = 3$ and we are in case (3) of the lemma. \square

The Ree group 2G_2 with $\ell = 2$ is a genuine counterexample since the Sylow 2-subgroups of ${}^2G_2(q)$ are isomorphic to $(\mathbb{Z}/2)^3$.

3. THE STRUCTURE OF THE SYLOW ℓ -SUBGROUPS

Definition 3.1. Let $\mathbf{G}, F, \mathbf{G}_1, \mathcal{P}$ and n be as in 2.13 and let $\ell \neq p$ be a prime number. We define $D(\ell)$ as the set of integers d such that for some $\Phi \in \mathcal{P}$ dividing $\Phi_d(x^n)$ we have $\ell | \Phi(q^n)$, where η is as in Definition 2.18.

The following proposition is [Enguehard, Théorème 1] when $\eta = 1$; we give here a shorter proof. Since [Enguehard] was written, Malle ([Malle, 5.14 and 5.19]) has published a proof of (2) below — thus implicitly of (1) also — when $\eta = 1$ (giving more, see Theorem 3.3).

Theorem 3.2. Assume in the situation of 3.1 that $D(\ell) \neq \emptyset$, or equivalently that $\ell || |\mathbf{G}^F|$. Then

- (1) $d(\ell) \in D(\ell)$.
- (2) There exists a unique $\Phi \in \mathcal{P}$ such that $\ell | \Phi(q^n)$ and Φ divides $\Phi_{d(\ell)}(x^n)$. If \mathbf{S} is a Sylow Φ -torus then $N_{\mathbf{G}}(\mathbf{S})$ contains a Sylow ℓ -subgroup of \mathbf{G}^F which is an extension of $(Z^0 C_{\mathbf{G}}(\mathbf{S}))_\ell^F$ by a Sylow ℓ -subgroup of W_Φ .
- (3) The Sylow ℓ -subgroups of \mathbf{G}^F are abelian if and only if $|D(\ell)| = 1$ (which is equivalent to W_Φ being an ℓ' -group), apart from the exception where

(\mathbf{G}_1, F_1) is of type 2G_2 and $\ell = 2$ in which case $|D(\ell)| = 2$ and $|W_\Phi| = 6$ but the 2-Sylow is abelian, isomorphic to $(\mathbb{Z}/2)^3$.

Further, if \mathbf{S} is as in (2), then $(Z^0 C_{\mathbf{G}}(\mathbf{S}))_\ell^F = \mathbf{S}_\ell^F$ except if:

- $\ell = 3$ and \mathbf{G}_1 of type 3D_4 .
- $\ell = 2, d = 1$ and for some odd degree $\varepsilon_i = -1$. Equivalently \mathbf{G}_1 is non-split and has an odd reflection degree, that is, is one of ${}^2A_n, {}^2D_{2n+1}$ or 2E_6 .
- $\ell = 2, d = 2$ and for some odd degree $\varepsilon_i = 1$; equivalently \mathbf{G}_1 is split and has an odd reflection degree, that is, is one of $A_n (n > 1), D_{2n+1}$ or E_6 .

In the above exceptions, $Z^0 C_{\mathbf{G}}(\mathbf{S}) = C_{\mathbf{G}}(\mathbf{S})$ is a maximal torus of \mathbf{G} .

Proof. Let us note that to prove (2) when we are not in an exception, that is the stronger statement that a Sylow ℓ -subgroup is in an extension of \mathbf{S}^F by a Sylow ℓ -subgroup of W_Φ , it is enough to prove that

$$v_\ell(|\mathbf{G}^F|) = v_\ell(|\mathbf{S}^F|) + v_\ell(|W_\Phi|) \quad (*)$$

where v_ℓ denotes the ℓ -adic valuation, and in the exceptions, if we have proved that $Z^0 C_{\mathbf{G}}(\mathbf{S}) = C_{\mathbf{G}}(\mathbf{S})$ it is enough to show

$$v_\ell(|\mathbf{G}^F|) = v_\ell(|C_{\mathbf{G}}(\mathbf{S})^F|) + v_\ell(|W_\Phi|) \quad (**)$$

Note also that by the definition of $d(\ell)$ and $D(\ell)$ in Proposition 2.13, assertion (1) as well as formulae (*) and (**) are equivalent in \mathbf{G} and \mathbf{G}_1 , that is we may assume \mathbf{G} quasi-simple to prove them which we do now. Also, in view of (2) and Proposition 2.19(4), (3) reduces to proving:

(3') $|D(\ell)| = 1$ is equivalent to W_Φ being an ℓ' -group.

We first look at the case of a Ree or Suzuki group, where $\eta = 2$.

Let us prove (1) first. By Lemma 4.2 if ℓ divides $|\mathbf{G}^F|$ then there is an element of $D(\ell)$ of the form $d(\ell)\ell^b$ with $b \geq 0$. By inspecting the order formula for $|\mathbf{G}^F|$ given in the proof of 2.11 the elements of $D(\ell)$ have all their prime factors in $\{2, 3\}$, so $b > 0$ implies $\ell \in \{2, 3\}$ thus $d(\ell) \in \{1, 2\}$; inspecting again the formula, we see that then $d(\ell)$ in $D(\ell)$ and that $|D(\ell)| = 1$ unless $\ell \in \{2, 3\}$.

To prove (2) for $\ell \notin \{2, 3\}$, we observe there is a single $\Phi \in \mathcal{P}$ such that $\ell | \Phi(q)$ since the two numbers $\Phi'_{2,4}(q), \Phi''_{2,4}(q)$ are prime to each other, and the same observation applies to $\Phi'_{2,6}(q), \Phi''_{2,6}(q)$ and $\Phi'_{2,12}(q), \Phi''_{2,12}(q)$. Thus for $\ell \notin \{2, 3\}$ assertions (3') and (*) are obvious since $|\mathbf{G}^F|_\ell = |\mathbf{S}^F|_\ell$ and $\ell \nmid |W|$.

Let us prove (*) for $\ell \in \{2, 3\}$; since $\ell \neq p$ and the elements of $D(\ell)$ have only 2 as prime factor in the case 2B_2 , we have just to consider:

- $\ell = 3$ for 2F_4 : we have $d(3) = 2$, $W_{\Phi_{2,2}} = G_{12}$ of order 48; the only factor $\Phi(q)$ with a value divisible by 3 apart from $|\mathbf{S}^F| = \Phi_{2,2}(q)^2$ is $\Phi_{2,6}(q)$ and $v_3(\Phi_{2,6}(q)) = 1 = v_3(|G_{12}|)$ which proves this case.
- $\ell = 2$ for 2G_2 : we have $d(2) = 2$ and $|W_{\Phi_{2,2}}| = 6$; the only factor $\Phi(q)$ with an even value apart from $|\mathbf{S}^F| = \Phi_{2,2}(q)$ is $\Phi_{2,1}(q)$ and $v_2(\Phi_{2,1}(q)) = 1 = v_2(|W_\Phi|)$ which proves this case.

We have seen (3') along the way.

Now we look at the other quasi-simple groups thus $\eta = 1$. We notice generally that, assuming we have proved (1) then if $|D(\ell)| = 1$ assertion (2) is trivial since a Sylow ℓ -subgroup is then in \mathbf{S} , and (3') reduces to checking that W_Φ is an ℓ' -group.

We consider separately 3D_4 where $|{}^3D_4(q)| = q^{12}(\Phi_1^2\Phi_2^2\Phi_3^2\Phi_6^2\Phi_{12})(q)$. Again, since the only prime factors of elements of $D(\ell)$ are $\{2, 3\}$, we see that $d(\ell) \in D(\ell)$

except possibly if $\ell \in \{2, 3\}$; but in that case $d(\ell) \in \{1, 2\}$ and there is a factor $\Phi_{d(\ell)}(q)$, whence (1). Since $|W| = 3 \cdot 2^6$ assertion (3') is proved when $D(\ell) = 1$. It remains to prove (2) when $\ell \in \{2, 3\}$. In both cases $W_{\Phi_{d(\ell)}} = W(G_2)$ and by Lemma 4.2 $v_\ell(|\mathbf{G}^F|/|\mathbf{S}^F|) = 2$. If $\ell = 2$ then $2 = v_\ell(|W(G_2)|)$ which proves (*). If $\ell = 3$ a Sylow Φ -subtorus \mathbf{S} is in a torus $\mathbf{T}_w = C_{\mathbf{G}}(\mathbf{S})$ where $w = 1$ if $d = 1$ (resp. $w = w_0$ if $d = 2$). We have $|\mathbf{T}_1^F| = \Phi_1(q)^2 \Phi_3(q)$ (resp. $|\mathbf{T}_{w_0}^F| = \Phi_2(q)^2 \Phi_6(q)$) which has same 3-valuation as $|\mathbf{G}^F|/|W_\Phi|$ which proves (**).

In the remaining cases $\varepsilon_i = \pm 1$ for all i . Let us set $\zeta_d = e^{2i\pi/d}$. We have $\Phi = \Phi_{d(\ell)}$ and $v_\ell(|\mathbf{S}^F|) = |a(\zeta_{d(\ell)})|v_\ell(\Phi_{d(\ell)}(q))$.

We first treat the case ℓ odd. We have $a(\zeta_d) = \{d_i \mid \zeta_d^{d_i} = \varepsilon_i\}$ and $|W_\Phi| = \prod_{d_i \in a(\zeta_{d(\ell)})} d_i$. By Lemma 4.2, a factor $\Phi_e(q)$ of $|\mathbf{G}^F|$ can contribute to the ℓ -valuation only if e is of the form $d(\ell)\ell^b$ for some $b \geq 0$. Further such a factor appears if and only if $a(\zeta_e) \neq \emptyset$, that is for some i we have $\zeta_{d(\ell)\ell^b}^{d_i} = \varepsilon_i$. Since ℓ is odd raising this equality to the power ℓ^b gives $\zeta_{d(\ell)}^{d_i} = \varepsilon_i$ thus $d_i \in a(\zeta_{d(\ell)})$ and in particular $d(\ell) \in D(\ell)$. And $\zeta_{d(\ell)\ell^b}^{d_i} = \varepsilon_i$ implies that ℓ^b divides d_i . Thus only the d_i in $a(\zeta_{d(\ell)})$ contribute to $v_\ell(|\mathbf{G}^F|)$ and each of them contributes $v_\ell(\Phi_{d(\ell)}(q)) + v_\ell(\Phi_{d(\ell)\ell}(q)) + \dots + v_\ell(\Phi_{d(\ell)\ell^{v_\ell(a_i)}}(q))$. By Lemma 4.2 this is $v_\ell(\Phi_{d(\ell)}(q)) + v_\ell(d_i)$. Summing over $d_i \in a(\zeta_{d(\ell)})$ proves (*).

It remains the case $\ell = 2$ where we proceed similarly. We have $d(2) \in \{1, 2\}$. If $d(2) = 1$ then $a(1) = \{d_i \mid \varepsilon_i = 1\}$. Thus the condition $\zeta_{2^b}^{d_i} = \varepsilon_i$ is still equivalent to $2^b \mid d_i$; but there could be some more solutions of this equation than elements of $a(1)$ when $b = 1$: any odd d_i such that $\varepsilon_i = -1$ brings an additional factor $1 = v_2(\Phi_2(q))$. If $d(2) = 2$ then $a(-1) = \{d_i \mid \varepsilon_i = (-1)^{d_i}\}$. The contribution of the even d_i can be worked out as before; but this time the odd d_i where $\varepsilon_i = 1$ bring additional factors $v_2(\Phi_1(q))$. In the exceptions in each case $C_{\mathbf{G}}(\mathbf{S})$ is a maximal torus of type 1 or w_0 ; looking at the orders of these tori, they contain enough extra Φ_1 or Φ_2 factors (which correspond to the eigenvalues 1 or -1 of ϕ or $w_0\phi$) to compensate the discrepancy.

Let us show now (3'), which reduces to proving that $|D(\ell)| > 1$ implies $v_\ell(|W_\Phi|) > 0$. Thus we assume $|D(\ell)| > 1$. We first do the case $\ell = 2$; then $d(\ell) \in \{1, 2\}$ from which it follows, since the 1 and -1 -eigenspaces are defined over the reals, that W_Φ is a Coxeter group, whose order is always even. We consider finally ℓ odd; then $D(\ell) \ni d(\ell)$ and $d(\ell)\ell^a$ for some $a > 0$. But we have seen above that there exists a factor $\Phi_{d(\ell)\ell^a}(q)$ only if $\ell^a \mid d_i$ for some d_i in $a(\zeta_{d(\ell)})$. \square

We remark that if ℓ divides only one $\Phi_d(q)$, a Sylow ℓ -subgroup S lies in a single Sylow Φ -torus \mathbf{S} (the intersection of two tori has lower dimension so cannot have same order polynomial). It follows that $N_{\mathbf{G}^F}(S) = N_{\mathbf{G}^F}(\mathbf{S})$ and $C_{\mathbf{G}^F}(S) = C_{\mathbf{G}^F}(\mathbf{S})$. This observation is a start for describing the ℓ -Frobenius category of \mathbf{G}^F in terms of the category of ζ_d -eigenspaces of W_{Φ_d} .

In general, one can deduce the following unicity theorem from the work of Cabanes, Enguehard and Malle.

Theorem 3.3. *Consider $\mathbf{G}, F, n, \mathbf{G}_1, q$ as in 2.13 with $q^n \in \mathbb{Z}$ and let Φ as defined in Theorem 3.2, (2). Assume that we are not in one of the following cases:*

- $\ell = 3$, \mathbf{G}_1 simply connected of type $A_2, {}^2A_2$ or G_2 .
- $\ell = 2$, \mathbf{G}_1 simply connected of type $C_n, n \geq 1$.

Let Q be a Sylow ℓ -subgroup of \mathbf{G}^F . There is a unique Sylow Φ -subtorus \mathbf{S} of \mathbf{G} such that $Q \subseteq N_{\mathbf{G}}(\mathbf{S})$.

Proof. In the context of Theorem 3.2(2), let Q be a Sylow ℓ -subgroup of \mathbf{G}^F contained in $N_{\mathbf{G}}(\mathbf{S})$; then according to [Cabanes], \mathbf{S}_{ℓ}^F is often characteristic in Q (for example when $\ell \geq 5$), thus in these cases $N_{\mathbf{G}^F}(Q) \subseteq N_{\mathbf{G}}(\mathbf{S}_{\ell}^F)$. Using inductively that property and inspecting small cases, G. Malle has proved the inclusion

$$(3.4) \quad N_{\mathbf{G}^F}(Q) \subseteq N_{\mathbf{G}}(\mathbf{S})$$

for all quasi-simple groups \mathbf{G} short of the cases excluded in Theorem 3.3, see [Malle, Theorems 5.14 and 5.19]. Here \mathbf{S} is a Sylow $\Phi_{d(\ell)}$ -subtorus of (\mathbf{G}, F) as defined in Definition 2.18 with $\eta = 1$ (note that $N_{\mathbf{G}^F}(Q) \subseteq N_{\mathbf{G}}(\mathbf{S})$ implies $Q \subseteq N_{\mathbf{G}}(\mathbf{S})$).

We first verify that the last inclusion holds more generally in a "descent of scalars". With hypotheses and notations of Proposition 2.13 and Lemma 2.14 assume $q^n \in \mathbb{Z}$. If $e = d(\ell)$ is the order of q^n modulo ℓ , take $\Phi = \Phi_e \in \mathcal{P}$, defining $\mathbf{S} = \mathbf{S}_{\Phi}$ and \mathbf{S}_1 . There is a morphism from \mathbf{G} onto \mathbf{G}_1 , sending \mathbf{S} to \mathbf{S}_1 , with restriction an isomorphism from \mathbf{G}^F to \mathbf{G}_1^F . Then a Sylow ℓ -subgroup Q_1 of \mathbf{G}_1^F contained in $N_{\mathbf{G}_1}(\mathbf{S}_1)$ is the isomorphic image of a Sylow ℓ -subgroup Q of \mathbf{G}^F contained in $N_{\mathbf{G}}(\mathbf{S})$. The inclusion 3.4 written with $(\mathbf{G}_1, F_1, Q_1, \mathbf{S}_1)$ instead of $(\mathbf{G}, F, Q, \mathbf{S})$ implies 3.4 in (\mathbf{G}, F) .

From 3.4 the unicity of \mathbf{S} , given Q , follows:

Lemma 3.5. *Let $\Phi \in \mathcal{P}$, let \mathbf{S} be a Sylow Φ -subtorus of (\mathbf{G}, F) and Q a Sylow ℓ -subgroup of \mathbf{G}^F . If $N_{\mathbf{G}^F}(Q) \subseteq N_{\mathbf{G}}(\mathbf{S})$, then \mathbf{S} is the unique Sylow Φ -torus of (\mathbf{G}, F) such that $Q \subseteq N_{\mathbf{G}}(\mathbf{S})$.*

Proof. Assume $Q \subseteq N_{\mathbf{G}}(\mathbf{S}')$ for some Sylow Φ -torus \mathbf{S}' of (\mathbf{G}, F) . By Proposition 2.19 there exists $g \in \mathbf{G}^F$ such that $\mathbf{S} = (\mathbf{S}')^g$, hence $Q^g \subseteq N_{\mathbf{G}}(\mathbf{S})$. By Sylow's theorem in $N_{\mathbf{G}}(\mathbf{S})^F$, $Q = Q^{gh}$ for some $h \in N_{\mathbf{G}}(\mathbf{S})^F$ hence $gh \in N_{\mathbf{G}}(\mathbf{S})$ by our hypothesis. \square

\square

4. APPENDIX

We gather here arithmetical lemmas used above.

Lemma 4.1. *Let $x, f, \ell \in \mathbb{N}$ where ℓ is prime, and assume $x \equiv 1 \pmod{\ell}$ (resp.*

$\pmod{4}$ if $\ell = 2$). Then $v_{\ell}(\frac{x^f - 1}{x - 1}) = v_{\ell}(f)$.

Proof. From $\frac{x^{f_1 f_2} - 1}{x - 1} = \frac{x^{f_1 f_2} - 1}{x^{f_2} - 1} \frac{x^{f_2} - 1}{x - 1}$ we see that it is enough to show the lemma when f is prime. We have $\frac{x^f - 1}{x - 1} = f + \sum_{i=2}^{f-1} (x - 1)^{i-1} \binom{f}{i}$. Let S be this last sum; we have $S \equiv f \pmod{\ell}$, since $x - 1 \equiv 0 \pmod{\ell}$, thus S is prime to ℓ when $f \neq \ell$ which shows the lemma in this case. When $f = \ell$ then all the terms of S but the first one and possibly the last one are divisible by ℓ^2 since $\binom{\ell}{i}$ is divisible by ℓ when $2 \leq i < \ell$; the last term is divisible by ℓ^2 when $\ell - 1 \geq 2$ which fails only for $f = \ell = 2$; but when $\ell = 2$ we have arranged that $v_{\ell}(x - 1) \geq 2$ and this time $2(f - 1) \geq 1$; thus $S \equiv f \pmod{\ell^2}$, whence the lemma. \square

The following lemma is in [Malle, 5.2]; a short elementary proof results immediately from Lemma 4.1.

Lemma 4.2. *Let $q, \ell \in \mathbb{N}$ where ℓ is prime. Let d be the order of $q \pmod{\ell}$ (or $\pmod{4}$ if $\ell = 2$). Then ℓ divides $\Phi_e(q)$ if and only if e is of the form $d\ell^b$ with $b \in \mathbb{N}$ (or additionally $b = -1$ when $\ell = d = 2$), and $v_\ell(\Phi_{d\ell^b}(q)) = 1$ if $b \neq 0$.*

The following lemma is in [Minkowski]; we give the proof since it is very short and the original German proof may be less accessible.

Lemma 4.3. *Let $m \in \mathbb{N}, m > 2$. Then the kernel of the reduction map $\mathrm{GL}(\mathbb{Z}^n) \rightarrow \mathrm{GL}((\mathbb{Z}/m)^n)$ is torsion-free.*

Note that the bound $m > 2$ is sharp since $-\mathrm{Id} \equiv \mathrm{Id} \pmod{2}$.

Proof. Let $w \in \mathrm{GL}(\mathbb{Z}^n)$ be of finite order, $w \neq \mathrm{Id}$ and assume its reduction $v = \mathrm{Id}$. We will derive a contradiction.

Possibly replacing w by a power, we may assume that w is of prime order p .

Also $\mathrm{GL}(\mathbb{Z}^n/m) = \prod_i \mathrm{GL}(\mathbb{Z}^n/p_i)$ where $m = \prod_i p_i$ is the decomposition of m into prime powers, thus we may assume that m is a prime power.

Since w is of order p , the polynomial $\Phi_p(x)$ is a factor of the characteristic polynomial of w . The characteristic polynomial of v is the reduction \pmod{m} of that of w , thus we must have $\Phi_p(x) \pmod{m} \equiv (x-1)^{p-1}$; in particular $\binom{p-1}{1} \equiv -1 \pmod{m}$ thus $m|p$ which implies $m = p$.

Write now $w = \mathrm{Id} + xm^a$ where $x \pmod{m} \not\equiv 0$ and $a \in \mathbb{N}$. Then the equation $w^m = \mathrm{Id}$ gives $\sum_{i=1}^m \binom{i}{m} x^i m^{ai} = 0$, which after dividing by m^{a+1} becomes $x = -\sum_{i=2}^m \binom{i}{m} x^i m^{a(i-1)-1}$ where all coefficients on the right-hand side are divisible by m (since $m \geq 3$), which contradicts $x \pmod{m} \not\equiv 0$. \square

REFERENCES

- [Borel] A. Borel, “Linear algebraic groups”, Springer GTM no. 126, 2nd ed. 1991.
- [Broué] M. Broué, “Introduction to complex reflection groups and their braid groups”, *Lecture Notes in Mathematics* **1988**, Springer-Verlag, Berlin, 2010.
- [Broué-Malle] M. Broué and G. Malle, “Théorèmes de Sylow génériques pour les groupes réductifs sur les corps finis”, *Math. Annalen* **292** (1992), 241–262.
- [Cabanes] M. Cabanes, “Unicité du sous-groupe abélien distingué maximal dans certains sous-groupes de Sylow”, *C.R.A.S.* **318** (1994), 889–894.
- [Enguehard] M. Enguehard, “Sur les groupes de Sylow des groupes réductifs finis”, unpublished notes of october 1992.
- [Gorenstein-Lyons] D. Gorenstein and R. Lyons, “The local structure of finite groups of characteristic 2 type”, *Memoirs of AMS* **42**, 1983.
- [Malle] G. Malle, “Height 0 characters of finite groups of Lie type”, *Representation theory* **11**(2007), 192–220.
- [Minkowski] H. Minkowski, “Zur Theorie der positiven quadratischen Formen”, *J. Crelle* **101** (1887), 196–202.
- [Steinberg] R. Steinberg, “Endomorphisms of linear algebraic groups”, *Memoirs of the A.M.S.* **80**, 1965.

E-mail address: `michel.enguehard@imj-prg.fr`

UNIVERSITÉ PARIS-DIDEROT

E-mail address: `jean.michel@imj-prg.fr`

UNIVERSITÉ PARIS-DIDEROT